Cryptography and Security Assignment 1

Chi Yin Wong
836872

Question 1

a. Confidentiality is likely to be the most important factor. Confidentiality refers to the need for private information to be disclosed from unauthorized individuals, as well as for the owner of the private information to have control over what information can be collected and stored and by whom. The COVID passport would require users to provide private, sensitive health related information. Furthermore, it requires that they disclose this information to venues they wish to enter. Moreover, it is difficult to guarantee that the information is only used for the disclosed purpose of checking vaccination status, and information may be kept for longer than necessary. Thus, the public is most likely concerned with confidentiality issues in regards to the COVID passport.

b. Integrity is unlikely to be an important factor. Integrity refers to the COVID passport performing its intended function, that is, to show that the passport holder is vaccinated. In this case, since the COVID passport stores information about vaccinations that can only be changed by the user if they do get vaccinated, integrity is unlikely to be of too much concern to the public.

c. Availability is unlikely to be the most important factor. Availability refers to the COVID passport working promptly, with no service denial to users that are authorized. In this case, since a COVID passport is a digital ID that is stored on your phone in a government supported application and server, it is unlikely that it would be unavailable for long periods of time.

Question 2

a. The decryption function can be written as

$$p = D_{(a,b)}(c) = a^{-1}(c - b) \; mod \; 27$$

For the decryption function to exist, a must have an inverse, so a must be relatively prime to 27. Thus, a must satisfy gcd(a,27) = 1 for the decryption function to exist. b can be any integer for the decryption function to exist.

b. We know that a must be chosen so that a and 27 are relatively prime because a must have an inverse. 27 is a prime number, so a can take 26 values since $\phi(p) = p - 1$ for any prime p. b can be any value from integers mod 27, so it can take 27 values. Thus, there are 26*27 = 702 possible keys for this scheme.

c. This cipher would be considered a monoalphabetic cipher. This is because this cipher has a single fixed substitution structure where each plaintext letter is mapped to a unique character of ciphertext for a given key, and plaintext and ciphertext have a one to one relationship.

d. One of the weaknesses of this cipher is that it preserves the frequency of characters used in the English language. Given a large amount of ciphertext, an attacker could exploit this weakness by analysing the frequency of letters in the ciphertext and then comparing them with the frequency of letters in everyday English language. The attacker could also look for ciphertext letters that are commonly used together and assume that they are digrams, two letter combinations that are commonly used together i.e. th, ch etc. To show how an attacker can retrieve the key, we use the following example.

   Consider a key where a = 5 and b = 10.

   The plaintext is p = TREE which has sequence 19, 17, 4, 4.

   The resulting ciphertext is YODD with a sequence of 24, 14, 3, 3.

   Suppose after a few guesses the attacker guesses that X = T and C = E by analysing the English language (since E and T are some of the most commonly used letters of the alphabet). Then the attacker can write the equations

$$19a + b \equiv 24 \; mod \; 27$$
$$4a + b \equiv 3 \; mod \; 27$$

   The attacker can then solve the two equations by using the extended Euclidean algorithm to find the multiplicative inverse of a and arrive at the values a = 5 and b = 10. Thus, the attacker has retrieved the key from the ciphertext.

e. Given an oracle that can output the encrypted ciphertext for any plaintext, we could easily find the key by inputting 2 random characters of the alphabet and obtaining their corresponding ciphertext. That is, you know c and p. Then you can write down 2 equations of the form c = (ap + b) mod 27 using the encryption algorithm. You can solve the system of equations to obtain values for a and b, thus giving you the key.

Question 3

a. Language chosen: python

```
def extendedGCD(a,n):
    #base case
    if a == 0:
        return n,0,1
    else:
        q = n//a
        r = n%a
        d,x,y = extendedGCD(r, a)
        return d,y-q*x,x
```

b. Language chosen: python

```
def modularInverse(a,n):
    d,x,y = extendedGCD(a,n)
    if d != 1:
        return print("modular inverse doesn't exist")
    inv = x%n
    return inv
```

c. Student number = 836872

$$836872^{-1}\ mod\ 16811891 = 7187128$$

Question 4

a.

The encryption function is given by

$$C = KP\ mod\ 41$$

The decryption function is given by

$$P = K^{-1}C\ mod\ 41$$

The inverse of K can be found by finding the adjoint of matrix K and dividing by the determinant of K. We use R to find the adjoint and determinant of matrix K. The adjoint of matrix K is

$$\begin{matrix} -43445 & -408646 & -239960 & 464771 & 54408 \\ 47505 & -31966 & -59885 & 91016 & -61532 \\ 17625 & -67980 & -9875 & 68905 & -32210 \\ -8235 & 380197 & 237495 & -515922 & 46544 \\ -6875 & 470100 & 271850 & -535150 & -52125 \end{matrix}$$

We can simplify because we are in modulo 41, so we perform modulo 41 division on all the elements in the matrix. The determinant of matrix K is -1303025 mod 41. We use similar steps as the adjoint matrix to get the determinant equal to 37. Below is some handwritten working to better illustrate the steps:

ASSIGNMENT 1 Q 4 a)

Determinant:

$$-1303025 \mod 41$$

$$= -4 \mod 41$$

$$= 37$$

Simplifying Adjoint matrix:

$$\begin{bmatrix} -26 & -40 & -28 & 36 & 1 \\ 27 & -27 & -25 & 37 & -32 \\ 36 & -2 & -35 & 25 & -25 \\ -35 & 4 & 23 & -19 & 9 \\ -28 & 35 & 20 & -18 & -14 \end{bmatrix} \mod 41$$

Convert the negatives to positives

$$\begin{bmatrix} 15 & 1 & 13 & 36 & 1 \\ 27 & 14 & 16 & 37 & 9 \\ 36 & 39 & 6 & 25 & 16 \\ 6 & 4 & 23 & 22 & 9 \\ 13 & 35 & 20 & 23 & 27 \end{bmatrix} \mod 41$$

now we have

$$K^{-1} = \frac{1}{37} \left[\text{adjoint} \right] \bmod 41$$

$$K^{-1} = 37^{-1} \left[\quad \right] \bmod 41$$

we find the multiplicative inverse of $37^{-1} \bmod 41$ using extended GCD:

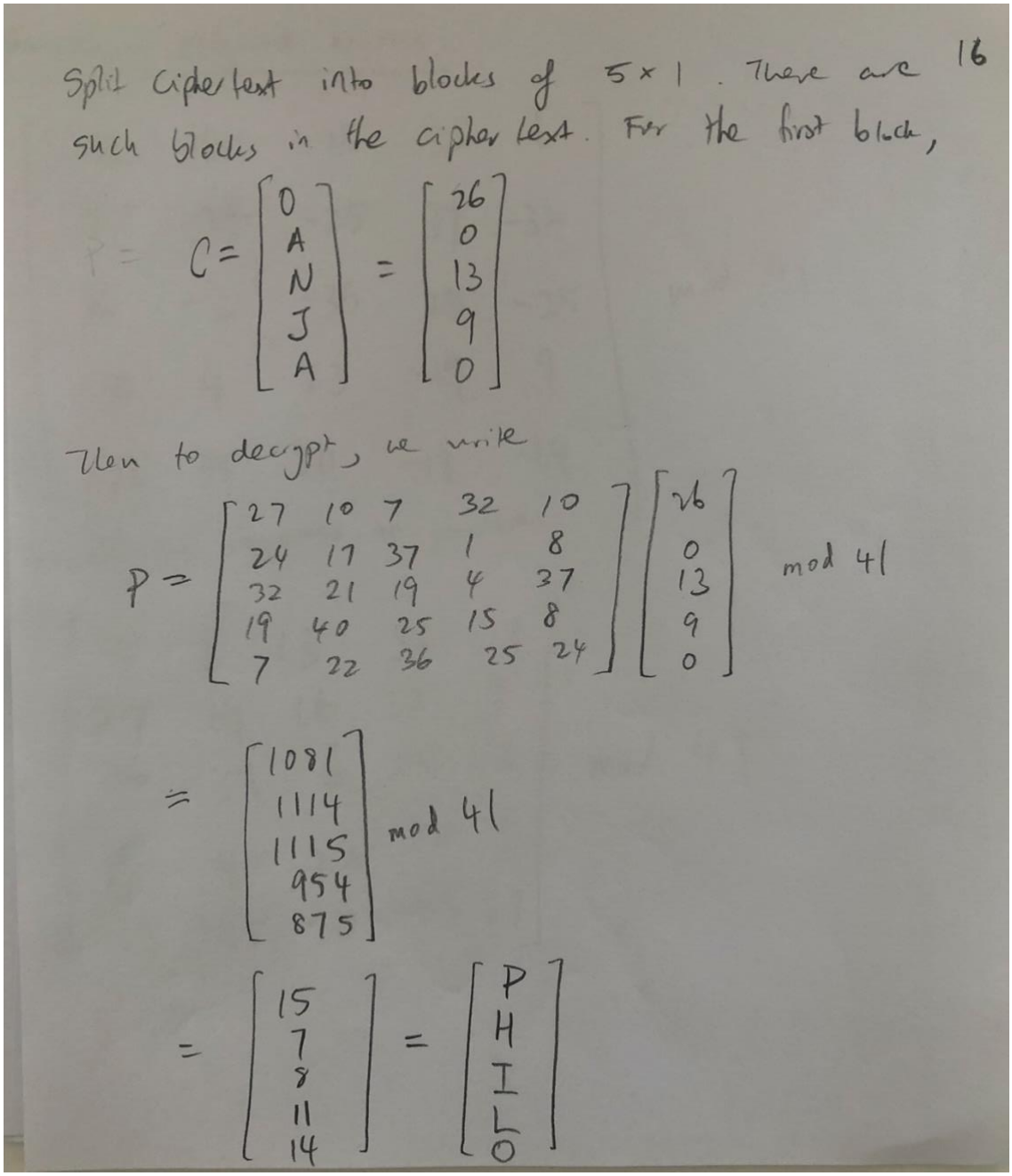
$$37^{-1} \bmod 41 = 10$$

$$\Rightarrow K^{-1} = 10 \begin{bmatrix} 15 & 1 & 13 & 36 & 1 \\ 27 & 14 & 16 & 37 & 9 \\ 36 & 39 & 6 & 25 & 16 \\ 6 & 4 & 23 & 22 & 9 \\ 13 & 35 & 20 & 23 & 27 \end{bmatrix} \bmod 41$$

$$= \begin{bmatrix} 150 & 10 & 130 & 360 & 10 \\ 270 & 140 & 160 & 370 & 90 \\ 360 & 390 & 60 & 250 & 160 \\ 60 & 40 & 230 & 220 & 90 \\ 130 & 350 & 200 & 230 & 270 \end{bmatrix} \bmod 41$$

$$K^{-1} = \begin{bmatrix} 27 & 10 & 7 & 32 & 10 \\ 24 & 17 & 37 & 1 & 8 \\ 32 & 21 & 19 & 4 & 37 \\ 19 & 40 & 25 & 15 & 8 \\ 7 & 22 & 36 & 25 & 24 \end{bmatrix}$$

Once the inverse of K has been obtained, we can easily decrypt the ciphertext by splitting the ciphertext into blocks of 5x1, converting it into its number representation from 0-40 and then multiplying the inverse of K to obtain the corresponding plaintext. We then convert the plaintext back into letters. We repeat this process for all 16 blocks to obtain the final plaintext. Below illustrates the first block (first five letters) of the ciphertext 0ANJA.



The final plaintext is

PHILOSOPHERS ASK CAN HUMAN INGENUITY CONCOCT A CIPHER WHICH HUMAN INGENUITY CANNOT RESOLVE 00

b. The number of possible keys for this Hill Cipher with a 5x5 key matrix is given by 41^{5*5}. Since 41 is a prime number, all the matrices will be invertible, thus the number of possible keys is

$$41^{5*5} = 208735548759234774491098559546826436810 01$$

For an alphabet with 38 characters, we have 38^{5*5}. However, not all the matrices will be invertible since 38 is not a prime number. 38 is made up of 2 prime numbers, 2 and 19. A matrix is invertible modulo a if it is also invertible modulo p, q where p and q are prime numbers and p*q = a. We can find the number of invertible n x n matrices modulo a with the formula

$$p^{n^2}\left(1-\frac{1}{p}\right)\left(1-\frac{1}{p^2}\right)\dots(1-\frac{1}{p^n})$$

The number of invertible 5x5 matrices modulo 2 is

$$2^{5^2}\left(1-\frac{1}{2}\right)\left(1-\frac{1}{2^2}\right)\dots\left(1-\frac{1}{2^5}\right) = 9999360$$

The number of invertible 5x5 matrices modulo 19 is

$$19^{5^2}\left(1-\frac{1}{19}\right)\left(1-\frac{1}{19^2}\right)\dots\left(1-\frac{1}{19^5}\right) = 8.7891994e^{31}$$

The number of invertible 5x5 matrices modulo 38 is given by the product of the above 2 equations, thus, the number of possible keys is approximately $8.791432e^{38}$.

c. Language used: R
Student number last 5 digits = 36872

The first step is to transform our ciphertext and plaintext into their corresponding integer values from 0 to 40.

Q.4

(c)

$$C = \begin{bmatrix} 40 \\ 22 \\ 16 \\ 36 \\ 35 \end{bmatrix} \qquad P = \begin{bmatrix} 23 \\ 24 \\ 40 \\ 11 \\ 4 \end{bmatrix}$$

Let $K = \begin{bmatrix} a & b & c & d & e \\ f & g & h & i & j \\ k & l & m & n & o \\ p & q & r & s & t \\ u & v & w & x & y \end{bmatrix}$

Then from the encryption function,

$$C = \begin{bmatrix} 40 \\ 22 \\ 16 \\ 36 \\ 35 \end{bmatrix} = \begin{bmatrix} a & b & c & d & e \\ f & g & h & i & j \\ k & l & m & n & o \\ p & q & r & s & t \\ u & v & w & x & y \end{bmatrix} \begin{bmatrix} 23 \\ 24 \\ 40 \\ 11 \\ 4 \end{bmatrix} = KP \bmod 41$$

we can repeat this for all 5 blocks. Next, we can build a system of equations for the first row of the key

$$40 = (23a + 24b + 40c + 11d + 4e) \bmod 41$$

$$1 = (17a + 31b + 7c + 8d + 37e) \bmod 41$$

$$34 = (36a + 11b + 12c + 14d + 15e) \bmod 41$$

$$16 = (16a + 17b + 29c + 32d + 34e) \bmod 41$$

$$27 = (33a + 28b + 18c + 1d + 9e) \bmod 41$$

This corresponds to the following matrix:

$$\begin{bmatrix} 40 \\ 1 \\ 34 \\ 16 \\ 27 \end{bmatrix} = \begin{bmatrix} 23 & 24 & 40 & 11 & 4 \\ 17 & 31 & 7 & 8 & 37 \\ 36 & 11 & 12 & 14 & 15 \\ 16 & 17 & 29 & 32 & 34 \\ 33 & 28 & 18 & 1 & 9 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ d \\ e \end{bmatrix}$$

We want to solve for a, b, c, d, e

To do this, we want to find the inverse of this matrix (call it A). Inverse of a matrix is given by $\frac{1}{|A|} \cdot \text{adjoint}(A)$.

The determinant of A $= 2557233 \bmod 41$
$= 22$

The adjoint of A modulo 41 =

$$\begin{bmatrix} 39 & 25 & 10 & 37 & 15 \\ 8 & 31 & 18 & 27 & 24 \\ 39 & 37 & 19 & 39 & 16 \\ 26 & 37 & 5 & 28 & 32 \\ 20 & 39 & 10 & 9 & 24 \end{bmatrix}$$

now we can write:

$$A^{-1} = \frac{1}{22} \cdot \text{adjoint}(A) \mod 41$$

we can take the multiplicative inverse of

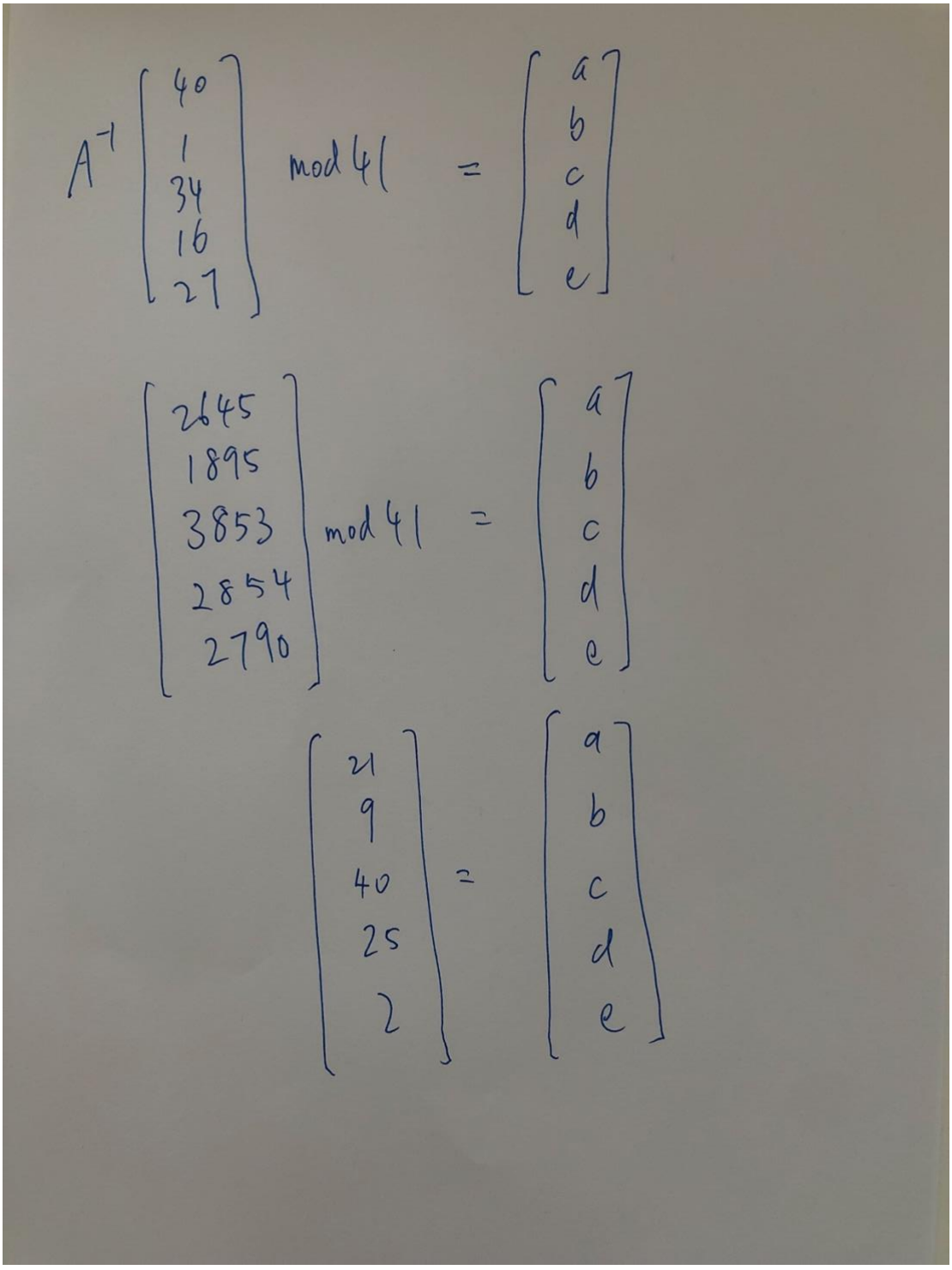
$22^{-1} \mod 41 = 28$.

$$A^{-1} = 28 \cdot \text{adjoint}(A) \mod 41$$

we multiply 28 and the adjoint matrix, and then take mod 41 to get

$$A^{-1} = \begin{bmatrix} 26 & 3 & 34 & 11 & 10 \\ 19 & 7 & 12 & 18 & 16 \\ 26 & 11 & 40 & 26 & 38 \\ 31 & 11 & 17 & 5 & 35 \\ 27 & 26 & 34 & 6 & 16 \end{bmatrix}$$

now we can multiply



Code for the first row of the key. This code was repeated for all the rows to obtain the encryption key matrix. The general procedure is demonstrated with the first row of the key, the process is repeated for all rows to get the key matrix.

```
# first row of the key
# finding the inverse of A
A = matrix(c(23,24,40,11,4,
             17,31,7,8,37,
```

```
        36,11,12,14,15,
        16,17,29,32,34,
        33,28,18,1,9),5,5, byrow = T)

adj.A = adjoint(A)
det.A = det(A)
det.A.mod41 = det(A)%%41

adj.A.mod41 = matrix(c(39,25,10,37,15,
                8,31,18,27,24,
                39,37,19,39,16,
                26,37,5,28,32,
                20,39,10,9,24),5,5,byrow = T)

det.A.multi.inverse = 28
inverse.A = det.A.multi.inverse*adj.A.mod41

inverse.A.mod41 = matrix(c(26,3,34,11,10,
                  19,7,12,18,16,
                  26,11,40,26,38,
                  31,11,17,5,35,
                  27,26,34,6,16),5,5,byrow = T)

w = matrix(c(40,1,34,16,27),5,1)

K1 = inverse.A%*%w
K1.mod41 = matrix(c(21,9,40,25,2))
```

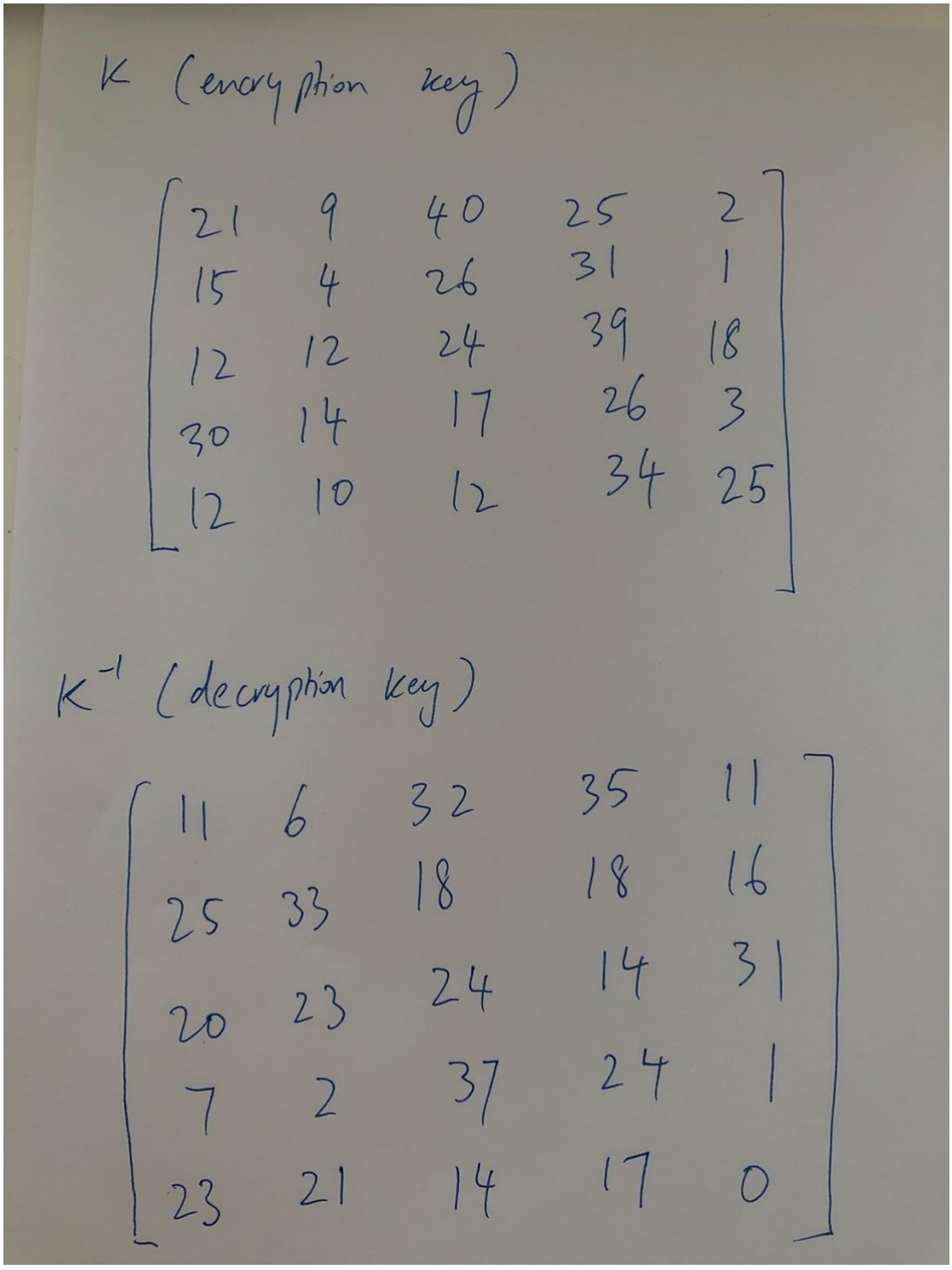
Thus the first row of the key is 21,9,40,25,2. Repeat this for the other plaintext-ciphertext pair blocks. The decryption key matrix is the inverse of the key matrix. To get the inverse of the key matrix, we do a similar process as above (and as in part a) by obtaining the determinant and adjoint of the key.

```
K = matrix(c(21,9,40,25,2,
        15,4,26,31,1,
        12,12,24,39,18,
        30,14,17,26,3,
        12,10,12,34,25),5,5,byrow = T)

adj.K = adjoint(K)
adj.K.mod41 = matrix(c(20,37,6,4,20,
                38,19,29,29,3,
                14,12,25,18,34,
                9,26,30,25,13,
                12,27,18,16,0),5,5,byrow=T)

det.K = det(K)
```

```
det.K.mod41 = det.K%%41
det.K.multi.inverse = 19
inverse.K = det.K.multi.inverse*adj.K.mod41
inverse.K.mod41 = matrix(c(11,6,32,35,11,
                           25,33,18,18,16,
                           20,23,24,14,31,
                           7,2,37,24,1,
                           23,21,14,17,0),5,5,byrow = T)
```



With the decryption key matrix, we can now decrypt the ciphertext by repeating our steps in part a. The final plaintext is

V7S9C HKTGM KY75R 3U9EP E[S9T VJSPR O2T[K [M=E[JT6M: 3FSY1 B5I[Z